chapter 3

Operational and Organizational Security

We will bankrupt ourselves in the vain search for absolute security.

—Dwight David Eisenhower

In this chapter, you will learn how to

- Identify various operational aspects to security in your organization
- Identify various policies and procedures in your organization
- Identify the security awareness and training needs of an organization
- Understand the different types of agreements employed in negotiating security requirements

Organizations achieve operational security through policies and procedures that guide users' interactions with data and data-processing systems. Developing and aligning these efforts with the goals of the business are crucial aspects of developing a successful security program. One method of ensuring coverage is to align efforts with the operational security model described in the last chapter. This breaks efforts into groups: prevention, detection, and response elements.

Prevention technologies are designed to keep individuals from being able to gain access to systems or data they are not authorized to use. Originally, this was the sole approach to security. Eventually we learned that in an operational environment, prevention is extremely difficult and relying on prevention technologies alone is not sufficient. This led to the rise of technologies to detect and respond to events that occur when prevention fails. Together, the prevention technologies and the detection and response technologies form the operational model for computer security.

Policies, Procedures, Standards, and Guidelines

The important parts of any organization's approach to implementing security include the policies, procedures, standards, and guidelines that are established to detail what users and administrators should be doing to maintain the security of the systems and network. Collectively, these documents provide the guidance needed to determine how security will be implemented in the organization. Given this guidance, the specific technology and security mechanisms required can be planned for.

Policies are high-level, broad statements of what the organization wants to accomplish. They are made by management when laying out the organization's position on some issue. **Procedures** are the step-by-step instructions on how to implement policies in the organization. They describe exactly how employees are expected to act in a given situation or to accomplish a specific task. **Standards** are mandatory elements regarding the implementation of a policy. They are accepted specifications that provide specific details on how a policy is to be enforced. Some standards are externally driven. Regulations for banking and financial institutions, for example, require certain security measures be taken by law. Other standards may be set by the organization to meet its own security goals. **Guidelines** are recommendations relating to a policy. The key term in this case is *recommendations*—guidelines are not mandatory steps.

Just as the network itself constantly changes, the policies, procedures, standards, and guidelines should be living documents that are periodically evaluated and changed as necessary. The constant monitoring of the network and the periodic review of the relevant documents are part of the process that is the operational model. When applied to policies, this process results in what is known as the *policy lifecycle.* This operational process and policy lifecycle roughly consist of four steps in relation to your security policies and solutions:

1. Plan (adjust) for security in your organization.
2. Implement the plans.
3. Monitor the implementation.
4. Evaluate the effectiveness.

In the first step, you develop the policies, procedures, and guidelines that will be implemented and design the security components that will protect your network. A variety of governing instruments—from standards to compliance rules—will provide boundaries for these documents. Once these documents are designed and developed, you can implement the plans. Part of the implementation of any policy, procedure, or guideline is an instruction period during which those who will be affected by the change or introduction of this new document can learn about its contents. Next, you monitor to ensure that both the hardware and the software, as well as the policies, procedures, and guidelines, are effective in securing your systems. Finally, you evaluate the effectiveness of the security measures you have in place. This step may include a *vulnerability assessment* (an attempt to identify and prioritize the list of vulnerabilities within a system

These documents guide how security will be implemented in the organization:

Policies High-level, broad statements of what the organization wants to accomplish

Procedures Step-by-step instructions on how to implement the policies

Standards Mandatory elements regarding the implementation of a policy

Guidelines Recommendations relating to a policy

or network) and a *penetration test* (a method to check the security of a system by simulating an attack by a malicious individual) of your system to ensure the security is adequate. After evaluating your security posture, you begin again with Step 1, this time adjusting the security mechanisms you have in place, and then continue with this cyclical process.

Regarding security, every organization should have several common policies in place (in addition to those already discussed relative to access control methods). These include, but are not limited to, security policies regarding change management, classification of information, acceptable use, due care and due diligence, due process, need to know, disposal and destruction of data, service level agreements, human resources issues, codes of ethics, and policies governing incident response.

Organizational Policies

The important parts of any organization's approach to implementing security include the policies, procedures, standards, and guidelines that are established to detail what users and administrators should be doing to maintain the security of the systems and network. Collectively, these documents provide the guidance needed to determine how security will be implemented in the organization. Given this guidance, the specific technology and security mechanisms required can be planned for.

Change Management Policy

The purpose of **change management** is to ensure proper procedures are followed when modifications to the IT infrastructure are made. These modifications can be prompted by a number of different events, including new legislation, updated versions of software or hardware, implementation of new software or hardware, and improvements to the infrastructure. The term *management* implies that this process should be controlled in some systematic way, and that is indeed the purpose. Changes to the infrastructure might have a detrimental impact on operations. New versions of operating systems or application software might be incompatible with other software or hardware the organization is using. Without a process to manage the change, an organization might suddenly find itself unable to conduct business. A change management process should include various stages, including a method to request a change to the infrastructure, a review and approval process for the request, an examination of the consequences of the change, resolution (or mitigation) of any detrimental effects the change might incur, implementation of the change, and documentation of the process as it relates to the change.

Change management is about the process of applying change. Change control is about the details of the change itself.

Change Control

Change control is the process of how changes to anything are sourced, analyzed, and managed. Change control is a subset of change management, focused on the details of a change and how it is documented.

Asset Management

Asset management involves the policies and processes used to manage the elements of the system, including hardware, software, and the data contained within them. In order to secure a system, one must have some form of control over these assets, and asset management involves the processes employed to keep the enterprise in positive control over these valuable items. Failures to control hardware can result in rogue network devices or computers accessing systems. Failure to control software can result in system-level vulnerabilities granting attackers free reign over a system and its data. Failure to control the data assets can result in many forms of failure. This makes asset management one of the most important aspects of security, and it is ranked at the top of virtually every standard list of controls.

Security Policies

In keeping with the high-level nature of policies, the **security policy** is a high-level statement produced by senior management that outlines both what security means to the organization and the organization's goals for security. The main security policy can then be broken down into additional policies that cover specific topics. Statements such as "this organization will exercise the principle of least access in its handling of client information" would be an example of a security policy. The security policy can also describe how security is to be handled from an organizational point of view (such as describing which office and corporate officer or manager oversees the organization's security program).

In addition to policies related to access control, the organization's security policy should include the specific policies described in the next sections. All policies should be reviewed on a regular basis and updated as needed. Generally, policies should be updated less frequently than the procedures that implement them, since the high-level goals will not change as often as the environment in which they must be implemented. All policies should be reviewed by the organization's legal counsel, and a plan should be outlined that describes how the organization will ensure that employees will be made aware of the policies. Policies can also be made stronger by including references to the authority who made the policy (whether this policy comes from the CEO or is a department-level policy, for example) and references to any laws or regulations applicable to the specific policy and environment.

Data Policies

System integration with third parties frequently involves the sharing of data. Data can be shared for the purpose of processing or storage. Control over data is a significant issue in third-party relationships. Numerous questions need to be addressed. For example, the question of who owns the data—both the data shared with third parties and subsequent data developed as part of the relationship—is an issue that needs to be established.

Tech Tip

Automation of Policy Enforcement

When you're making policies, there are some important questions you need to have answers for: How do you plan to enforce the policy? Should you even have a policy if there's no way to know who isn't following it? Maybe you want the policy just so that you can fire people you happen to catch after the fact (generally a bad idea). The keys to good policies are they support the desired work, they are relatively transparent (they don't impede work), and they are perceived as being fairly enforced. Automation is a key element, because if you know the states, both desired and prohibited, and can measure these with automation, then many of the desired elements can be achieved. Assume that certain functions are not to be used in coding—you can write filters to screen for these on code check-in, thus enforcing compliance with the approved functions policy. If you have something less defined, such as adding security usability tenets to the software development process, this is great as a guideline, but how would you specifically define it or enforce it on projects? The scale could be a problem, there's no way to automate it, and it is subjective—all of which results in uncertain outcomes and uneven enforcement. If you can define a way to automate the policy, this provides a lot of good data on whether it meets many of the goals associated with good policies.

Data Ownership

Data requires a data owner. Data ownership roles for all data elements need to be defined in the business. Data ownership is a business function, where the requirements for security, privacy, retention, and other business functions must be established. Not all data requires the same handling restrictions, but all data requires these characteristics to be defined. This is the responsibility of the data owner.

Besides data owners, there are data controllers, processors, and custodians/stewards. Each of these has responsibilities to protect data, and these responsibilities should be guided by policies.

Unauthorized Data Sharing

Unauthorized data sharing can be a significant issue, and in today's world, data has value and is frequently used for secondary purposes. Ensuring that all parties in the relationship understand the data-sharing requirements is an important prerequisite. Equally important is ensuring that all parties understand the security requirements of shared data.

Data Backups

Data ownership requirements include backup responsibilities. Data backup requirements include determining the level of backup, the restore objectives, and the level of protection requirements. These can be defined by the data owner and then executed by operational IT personnel. Determining the backup responsibilities and developing the necessary operational procedures to ensure that adequate backups occur are important security elements.

Classification of Information

A key component of IT security is the protection of the information processed and stored on the computer systems and network. Organizations deal with many different types of information, and they need to recognize that not all information is of equal importance or sensitivity. This requires classification of information into various categories, each with its own requirements for its handling. Factors that affect the classification of specific information include its value to the organization (what will be the impact to the organization if this information is lost?), its age, and laws or regulations that govern its protection. The most widely known system of classification of information is the one implemented by the U.S. government (including the military), which classifies information into categories such as *Confidential, Secret,* and *Top Secret.* Businesses have similar desires to protect information and often use categories such as *Publicly Releasable, Proprietary, Company Confidential,* and *For Internal Use Only.* Each policy for the classification of information should describe how it should be protected, who may have access to it, who has the authority to release it (and how), and how it should be destroyed. All employees of the organization should be trained in the procedures for handling the information they are authorized to access. Discretionary and mandatory access control techniques use classifications as a method to identify who may have access to what resources.

Tech Tip

Data Classification

Information classification categories you should be aware of for the CompTIA Security+ exam include High, Medium, Low, Confidential, Private, and Public.

Data Labeling, Handling, and Disposal

Effective data classification programs include data labeling, which enables personnel working with the data to know whether it is sensitive and to understand the levels of protection required. When the data is inside an information-processing system, the protections should be designed into the system. But when the data leaves this cocoon of protection, whether by printing, downloading, or copying, it becomes necessary to ensure continued protection by other means. This is where data labeling assists users in fulfilling their responsibilities. Training to ensure that labeling occurs and that it is used and followed is important for users whose roles can be impacted by this material.

Training plays an important role in ensuring proper data handling and disposal. Personnel are intimately involved in several specific tasks associated with data handling and data destruction/disposal. If properly trained, they can act as a security control. Untrained or inadequately trained personnel will not be a productive security control and, in fact, can be a source of potential compromise.

Governance

Data *governance* is the process of managing the availability, usability, integrity, and security of the data in enterprise systems. This must be done by policy, as it involves a large number of data owners and users. Data governance should have established data standards and policies that control data usage, security, and retention. Effective governance ensures that data usage is consistent with policies, that data elements are trustworthy, and that data doesn't get misused. The roles and responsibilities of those involved in data governance are covered in Chapter 25.

Retention

Data *retention* is the management of the data lifecycle with an emphasis on when data reaches the end of useful life for an organization. Maintaining old, excess data that no longer serves a business purpose only represents system risk and thus should be removed from the system and properly destroyed. Having a coordinated data retention policy is more than just labeling how long different types of data should be stored. Some types of data, financial records, tax records, and so on have specific regulatory requirements as to how long they must be maintained. The retention policy must also take into account things like legal holds (sometimes referred to as litigation holds) on specific data elements, suspending the destruction of those elements, and other regulatory concerns. Developing a data retention policy is relatively easy, but implementing it in an efficient and effective manner can be significantly more challenging given the diverse nature of data across the enterprise and the challenge presented by item-specific litigation holds.

A legal hold is a court directive to keep all records associated with a subject of a legal proceeding, and this order takes precedence over normal data retention policies.

Need to Know

Another common security principle is that of *need to know,* which goes hand-in-hand with *least privilege.* The guiding factor here is that each individual in the organization is supplied with only the absolute minimum amount of information and privileges they need to perform their work tasks.

The principle of least privilege states that users should only have a level of access permissions necessary to perform their assigned tasks.

To obtain access to any piece of information, the individual must have a justified need to know. A policy spelling out these two principles as guiding philosophies for the organization should be created. The policy should also address who in the organization can grant access to information and who can assign privileges to employees.

Disposal and Destruction Policy

Many potential intruders have learned the value of dumpster diving. An organization must be concerned about not only paper trash and discarded objects but also the information stored on discarded objects such as computers. Several government organizations have been embarrassed when old computers sold to salvagers proved to contain sensitive documents on their hard drives. It is critical for every organization to have a strong *disposal and destruction policy* and related procedures.

Important papers should be shredded, and *important* in this case means anything that might be useful to a potential intruder. It is amazing what intruders can do with what appear to be innocent pieces of information.

Before magnetic storage media (such as disks or tapes) is discarded in the trash or sold for salvage, it should have all files deleted and should be overwritten at least three times with all 1's, all 0's, and then random characters. Commercial products are available to destroy files using this process. It is not sufficient simply to delete all files and leave it at that, because the deletion process affects only the pointers to where the files are stored and doesn't actually get rid of all the bits in the file. This is why it is possible to "undelete" files and recover them after they have been deleted.

A safer method for destroying files from a storage device is to destroy the data magnetically, using a strong magnetic field to *degauss* the media. This effectively destroys all data on the media. Several commercial degaussers are available for this purpose. Another method that can be used on hard drives is to use a file on them (the sort of file you'd find in a hardware store) and actually file off the magnetic material from the surface of the platter. There are many means for storing data externally, from optical drives to USB sticks. In the case of optical discs (CDs, DVDs, and even Blu-ray discs), many paper shredders now have the ability to shred this form of storage media. In some highly secure environments, the only acceptable method of disposing of hard drives and other storage devices is the actual physical destruction of the devices. Matching the security action to the level of risk is important to recognize in this instance. Destroying hard drives that do not have sensitive information is wasteful; proper file scrubbing is probably appropriate. For drives with ultra-sensitive information, physical destruction makes sense. There is no single answer, but as in most things associated with information security, the best practice is to match the action to the level of risk. Data destruction is covered in detail in Chapter 25.

Credential Policies

Credential policies refer to the processes, services, and software used to store, manage, and log the use of user credentials. User-based credential management solutions are typically aimed at assisting end users in managing their growing set of passwords. There are credential management products that provide a secure means of storing user credentials and making

them available across a wide range of platforms, from local stores to cloud storage locations. System credential management solutions offer the same advantages to system owners, providing a means to manage who is given access to differing resources across the enterprise.

The key method used to control access to most systems is still one based on passwords. In conjunction with a strongly enforced account policy that prohibits the sharing of passwords and credentials, the use of passwords forms the foundation to support the concept that each user ID should be traceable to a single person's activity. Passwords need to be managed to provide appropriate levels of protection. They need to be strong enough to resist attack, and yet not too difficult for users to remember. An account policy can act to ensure that the necessary steps are taken to enact a secure password solution, both by users and by the password infrastructure system.

Personnel

Users, or *personnel,* require credentials to access specific system resources as part of their job duties. Management of who gets what credentials is part of the access and authorization management system and should be managed via a credential policy. The details behind credentials and policies for access control are covered in Chapter 11.

Third Party

Just as users inside a firm require credentials to access systems, there are situations where third parties also require credentials. Whether credentials for a system or physical access, *third-party* credentials should be managed by policies to ensure they are issued when needed to the correct parties, and when access is no longer needed, they are revoked appropriately.

Devices

Devices are physical items that require access to a network or enterprise system. To have this access, they require credentials just like human users. Unlike human users, devices do not have the ability to change their password, so they are typically enabled with very long passwords to prevent hacking and have longer-than-normal password expiration periods. This makes device accounts natural targets for attackers; while their long passwords may not be crackable, they can be stolen. Device accounts should be controlled by policy and monitored as to scope of use. Mobile device management policies are covered in detail in Chapter 12.

Service Accounts

Service accounts are special accounts that are used to provision permissions for services, or non-human-initiated system activity. Many computer systems have automated services that function as either part of, in addition to, the operating system to enable certain functionalities. These special programs require permissions like all programs that operate, and service accounts are the mechanism used to enable these items to run. Service accounts require auditing and oversight because they run in the background and frequently have significant capabilities. The enterprise needs a policy to determine who can enable and operate these accounts as well as their audit functions.

Because device and service accounts do not have human operators using them, their passwords have special properties, including very long expiration periods. They also commonly are employed to run processes at elevated levels of privilege. This makes them more susceptible to abuse, so their scope and usage should be monitored.

Administrator/Root Accounts

Administrators and root accounts have elevated privileges and require closer scrutiny as to who is issued these credentials and how they are used and monitored. Detailed information concerning the additional safeguards needed for these accounts is detailed in Chapter 11.

Tech Tip

What Makes a Usable Strong Password

New research from the National Institute of Standards and Technology (NIST) indicates that password complexity rules that are designed to force entropy into passwords do so at the risk of other, less-desired password behaviors, such as writing passwords down or versioning them with an increasing number element. The latest guidance is that long passphrases offer the best protection, but for the exam you should know the tried-and-true complexity requirements.

Password and Account Policies

Passwords are as ubiquitous as users; in fact, more so. The average user has more than 20 passwords in today's online environment. It seems that every site you go to wants you to log in and create a password. So if passwords are everywhere, why do we need a policy? Because passwords are important, and improper use and/or control over passwords is a leading cause of account hijacking. Policies can set expectations for the workforce as to what is needed in the form of passwords from a security perspective.

Password Complexity

Passwords must meet the defined *password complexity* requirements in the organization. Typically these requirements specify that the password must be a minimum length and have characters from at least three of the following four groups: English uppercase characters (*A* through *Z*), English lowercase characters (*a* through *z*), numerals (0 through 9), and non-alphabetic special characters (such as !, $, #, and %).

Account Expiration

Account expiration should occur when a user is no longer authorized to use a system. This requires coordination between those who manage the accounts and those who manage the need for access. The best solution is for the managers of the workers requiring access to manage the need—they are close to the situation, understand the need, and are generally the first to know when access is no longer necessary (for example, when an employee transfers or quits). These managers should be the first ones to notify the security team as to any changes in permissions, and human resources (HR) should play a backup role. Having frontline management initiate permissions issues also enables the proper continuation of permissions when a person departs. Who assumes ownership over files the previous person was sole owner of? This is a business decision and best managed by those closest to the business.

In Windows systems, user account expiration is a built-in feature that allows you to create a temporary user account that will expire automatically on the specified dates. Upon reaching the expiration date, the user account is expired and the user is unable to log on to Windows after that date. This can be good for temporary and contract workers.

Account Recovery

Account recovery seems like an esoteric topic until you lose the password on your laptop and have no way back in. This is even more serious if you lose administrator account passwords to key elements of your infrastructure. Having a recovery plan for accounts in case something happens to the

people who know the passwords is important in order for the enterprise to continue after the loss of a resource. Rather than focus on all the ways the organization can lose a resource—being fired, leaving on one's own accord, stepping in front of a bus, and so on—focus instead on a simple recovery method like an envelope containing a list of accounts and passwords, put in a safe governed by a different senior executive. Public key infrastructure (PKI) systems have key-recovery mechanisms that are there for a reason—to be used when emergencies happen. Account recovery is no different: you need to have a plan and execute it in order to prepare for an emergency when you need to put the plan into action. If you wait until you need a plan, it is too late to create it.

Account Disablement

Account disablement is the step between the account having access and the account being removed from the system. Whenever an employee leaves a firm, all associated accounts should be disabled to prevent further access. Disabling is preferable to removal because removal might result in permission and ownership problems. Periodic audits of user accounts to ensure they still need access is also a good security measure. Disabling an account is reversible, but it prohibits the account from being used until the issue that resulted in the disabling is resolved. Account disablement can be an automatic response from a security system if there is evidence that the account is under attack (say, from a brute force password attack).

Accounts have many facets that are governed by both action and policy. Remember, policy directs actions, and the specifics of the question give the context by which you can choose the best answer. There is a lot of detail in this section, and can be relevant in use.

Account Lockout

Account lockout is akin to disablement, although *lockout* typically refers to the ability to log on. If a user mistypes their password a certain number of times, they may be forced to wait a set amount of time while their account is locked before attempting to log in again. These lockouts can be automated on most systems and provide a series of increasing hurdles for an attacker, while minimizing the inconvenience to legitimate users who have credential problems.

Password History

Password history is a reference to previously used passwords by an account. It is good security policy to prohibit the reusing of passwords at least for a set number of previous passwords. In Windows, under Local Group Policy, you can set three elements that work together to manage password history:

- **Enforce password history** Tells the system how many passwords to remember and does not allow a user to reuse an old password.
- **Maximum password age** Specifies the maximum number of days a password may be used before it must be changed.
- **Minimum password age** Specifies the minimum number of days a password must be used before it can be changed again.

The minimum password age is used to prevent a user from changing their password 20 times in a row to recycle back to the previous or current password. Figure 3.1 shows password settings under Local Security Policy in Windows.

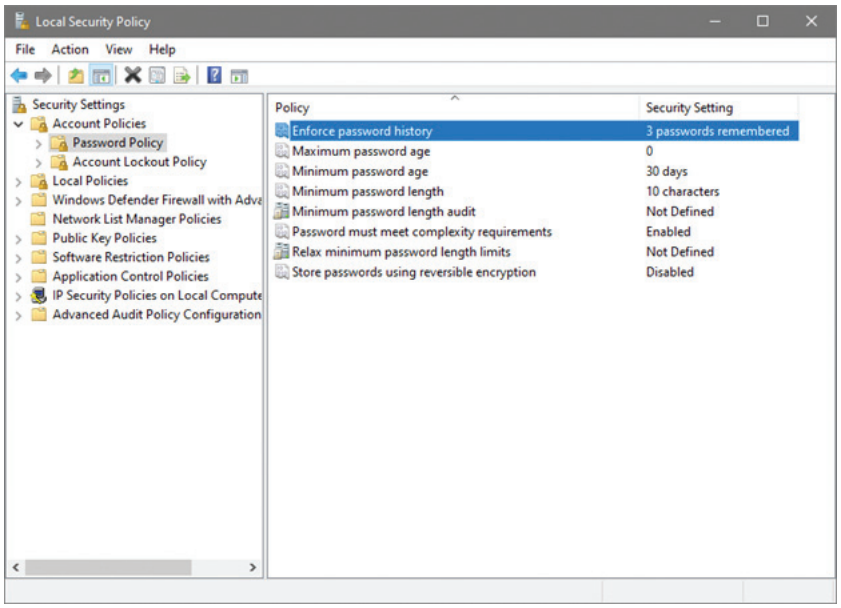

Figure 3.1 Password options under Local Security Policy settings in Windows

Password Reuse

Password reuse is a bad idea in that it reopens the organization to exposure from an adversary who has previously obtained a password. Passwords should not be reused for at least a year, and for at least a half dozen changes, whichever comes last. This is to minimize the opportunity for an adversary to take advantage of a reuse case.

Password Length

Password length is critical to password-based security. The true strength of a password lies in its entropy or randomness. The longer the entropy or randomness, the greater the keyspace that must be searched for random matching. Increasing password length and complexity is the easiest way to increase entropy in a password. Recent research has shown that passphrases, 20 characters or more, are easier to remember, are not typically written down, and can provide the required entropy to be effective. The only problem is not all systems take passphrases. That being said, the current standard is at least 10 characters with numbers, mixed-case, and special characters, and a length of 12 characters is preferred.

Protection of Passwords

The policy should stress not writing down passwords where others can find them, not saving passwords and not allowing automated logins, not sharing passwords with other users, and so on. Also, the consequences associated with violation of or noncompliance with the policy, or any part thereof, should be explained.

Human Resources Policies

It has been said that the weakest links in the security chain are humans. Consequently, it is important for organizations to have policies in place relative to their employees. Policies that relate to the hiring of individuals are primarily important. The organization needs to make sure it hires individuals who can be trusted with the organization's data and that of its clients. Once employees are hired, they should be kept from slipping into the category of "disgruntled employee." Finally, policies must be developed to address the inevitable point in the future when an employee leaves the organization—either on their own or with the "encouragement" of the organization itself. Security issues must be considered at each of these points.

Many organizations overlook the security implications that decisions by HR may have. HR personnel and security personnel should have a close working relationship. Decisions on the hiring and firing of personnel have direct security implications for the organization. As a result, procedures should be in place that specify which actions must be taken when an employee is hired, is terminated, or retires.

Code of Ethics

Numerous professional organizations have established codes of ethics for their members. Each of these describes the expected behavior of their members from a high-level standpoint. Businesses can adopt this idea as well. A code of ethics can set the tone for how employees will be expected to act and conduct business. The code should demand honesty from employees and require that they perform all activities in a professional manner. The code could also address principles of privacy and confidentiality and state how employees should treat client and organizational data. Conflicts of interest can often cause problems, so this could also be covered in the code of ethics.

By outlining a code of ethics, the organization can encourage an environment that is conducive to integrity and high ethical standards. For additional ideas on possible codes of ethics, check professional organizations such as the Institute for Electrical and Electronics Engineers (IEEE), the Association for Computing Machinery (ACM), and the Information Systems Security Association (ISSA).

Job Rotation

An interesting approach to enhancing security that is gaining increased attention is **job rotation**. Organizations often discuss the benefits of rotating individuals through various jobs in an organization's IT department. By rotating through jobs, individuals gain a better perspective on how the various parts of IT can enhance (or hinder) the business. Since security is often a misunderstood aspect of IT, rotating individuals through security positions can result in a much wider understanding throughout the organization about potential security problems. It also can have the side benefit of a company not having to rely on any one individual too heavily for security expertise. If all security tasks are the domain of one employee, and that individual leaves suddenly, security at the organization could suffer. On the other hand, if security tasks are understood by many different individuals, the loss of any one individual has less of an impact on the organization.

Rotating tasks between users reduces the risk that fraudulent activity can either go undetected or be sustained, and it improves security awareness across various roles in an organization.

Another aspect of the separation of duties principle is that it spreads responsibilities out over an organization so no single individual becomes the indispensable individual with all the "keys to the kingdom" or unique knowledge about how to make everything work. If enough tasks have been distributed, assigning a primary and a backup person for each task will ensure that the loss of any one individual will not have a disastrous impact on the organization.

Separation of Duties

Separation of duties is a principle employed in many organizations to ensure that no single individual has the ability to conduct transactions alone. This means that the level of trust in any one individual is lessened, and the ability for any individual to cause catastrophic damage to the organization is also lessened. An example might be an organization in which one person has the ability to order equipment, but another individual makes the payment. An individual who wants to make an unauthorized purchase for their own personal gain would have to convince another person to go along with the transaction.

Separating duties as a security tool is a good practice, but it is possible to go overboard and break up transactions into too many pieces or require too much oversight. This results in inefficiency and can actually be less secure, since individuals might not scrutinize transactions as thoroughly because they know others will also be reviewing them. The temptation is to hurry something along and assume that somebody else will examine it or has examined it.

Tech Tip

Hiring Hackers

Hiring a skilled hacker may make sense from a technical skills point of view, but an organization also has to consider the broader ethical and business consequences and associated risks. Is the hacker completely reformed or not? How much time is needed to determine this? The real question is not "would you hire a hacker?" but rather "can you fire a hacker once they have had access to your systems?" Trust is an important issue with employees who have system administrator access, and the long-term ramifications need to be considered.

Employee Hiring (Onboarding) and Promotions

It is becoming common for organizations to run background checks on prospective employees and to check the references prospective employees supply. Frequently, organizations require drug testing, check for any past criminal activity, verify claimed educational credentials, and confirm reported work history and even social media behavior. For highly sensitive environments, special security background investigations can also be required. Make sure that your organization hires the most capable and trustworthy employees, and that your policies are designed to ensure this.

After an individual has been hired, your organization needs to minimize the risk that the employee will ignore company rules and affect security. Periodic reviews by supervisory personnel, additional drug checks, and monitoring of activity during work may all be considered by the organization. If the organization chooses to implement any of these reviews, this must be specified in the organization's policies, and prospective employees should be made aware of these policies before being hired. What an organization can do in terms of monitoring and requiring drug tests, for example, can be severely restricted if not spelled out in advance as terms of employment. New hires should be made aware of all pertinent policies, especially those applying to security, and should be asked to sign documents indicating that they have read and understood them.

Tech Tip

Accounts of Former Employees

When conducting security assessments of organizations, security professionals frequently find active accounts for individuals who no longer work for the company. This is especially true for larger organizations, which may lack a clear offboarding process for the personnel office to communicate with the network administrators when an employee leaves the organization. These old accounts, however, are a weak point in the security perimeter for the organization and should be disabled or eliminated.

Occasionally an employee's status will change within the company. If the change can be construed as a negative personnel action (such as a demotion), supervisors should be alerted to watch for changes in behavior that might indicate the employee is contemplating or conducting unauthorized activity. It is likely that the employee will be upset, and whether they act on this to the detriment of the company is something that needs to be guarded against. In the case of a demotion, the individual may also lose certain privileges or access rights, and these changes should be made quickly so as to lessen the likelihood that the employee will destroy previously accessible data if they become disgruntled and decide to take revenge on the organization. On the other hand, if the employee is promoted, privileges may still change, but the need to make the change to access privileges might not be as urgent, though it should still be accomplished as quickly as possible. If the move is a lateral one, changes may also need to take place, and again they should be accomplished as quickly as possible.

A key element when **onboarding** personnel to any position, via hiring and promotions, is to ensure that the personnel are aware of and understand their responsibilities with respect to securing company information and the assets they will be using. Agreements with business partners tend to be fairly specific with respect to terms associated with mutual expectations associated with the process of the business. It should be the same with employees; ensuring the correct security elements are covered during onboarding is essential to setting proper employee expectations. These considerations need to be made prior to the establishment of the relationship, not added at the time that it is coming to an end.

Onboarding policy should include provisions for the handling of data, the disposal of data, acceptable use, and any sanctions that may occur as a result of misuse.

Retirement, Separation, or Termination (Offboarding)

Offboarding refers to the processes and procedures used when an employee leaves an organization. From a security perspective, the offboarding process for personnel is very important. Employee termination needs to be modified to include termination or disablement of all accounts, including those enabled on mobile devices. It's not uncommon to find terminated employees with accounts or even company devices still connecting to the corporate network months after being terminated.

Onboarding and offboarding procedures should be well documented to ensure compliance with legal requirements.

An employee leaving an organization can be either a positive or a negative action. Employees who are retiring by their own choice may announce their planned retirement weeks or even months in advance. Limiting their access to sensitive documents the moment they announce their intention may be the safest thing to do, but it might not be necessary or make business sense. Each situation should be evaluated individually. If the situation is a forced retirement, the organization must determine the risk to its data if the employee becomes disgruntled as a result of the action. In this situation, the wisest choice might be to cut off the employee's access quickly and provide them with some additional vacation time. This might seem like an expensive proposition, but the danger to the company of having a disgruntled employee may justify it. Again, each case should be evaluated individually.

It is better to give a potentially disgruntled employee several weeks of paid vacation than to have them trash sensitive files to which they have access. Because employees typically know the pattern of management behavior with respect to termination, doing the right thing will pay dividends in the future for a firm.

Organizations commonly neglect to have an offboarding policy that mandates the removal of an individual's computer access upon termination. Not only should such a policy exist, but it should also include the procedures to reclaim and "clean" a terminated employee's computer system and accounts.

When an employee decides to leave a company, generally as a result of a new job offer, continued access to sensitive information should be carefully considered. If the employee is leaving as a result of hard feelings toward the company, it might be wise to quickly revoke their access privileges.

If the employee is leaving the organization because they are being terminated, you should assume that they are or will become disgruntled. Although it might not seem the friendliest thing to do, you should immediately revoke their access privileges to sensitive information and facilities in this situation.

Combinations should also be quickly changed once an employee has been informed of their termination. Access cards, keys, and badges should be collected; the employee should be escorted to their desk and watched as they pack personal belongings, and then they should be escorted from the building. E-mail accounts should be disabled promptly as part of the employee termination policy and process. Mobile devices supplied by the company should be collected upon termination. Bring-your-own-device (BYOD) equipment should have its access to corporate resources terminated as part of the offboarding process. Regular audits for old or unterminated accounts should be performed to ensure prompt deletion or disablement of accounts for terminated employees.

Exit Interviews

Exit interviews can be powerful tools for gathering information when people leave a firm. From a security perspective, the offboarding process for personnel is very important. Employee termination needs to be modified to include termination of all accounts, including those enabled on mobile devices. It's not uncommon to find terminated employees with accounts or even company devices still connecting to the corporate network months after being terminated.

Don't forget business partners! Onboarding and offboarding business partners should be well documented to ensure compliance with legal requirements.

Onboarding/Offboarding Business Partners

Just as it is important to manage the on- and offboarding processes of company personnel, it is important to consider the same types of elements when making arrangements with third parties. Agreements with business partners tend to be fairly specific with respect to terms associated with mutual expectations associated with the process of the business. Considerations regarding the onboarding and offboarding processes are important, especially the offboarding. When a contract arrangement with a third party comes to an end, issues as to data retention and destruction by the third party need to be addressed. These considerations need to be made prior to the establishment of the relationship, not added when it is coming to an end.

Adverse Actions

Adverse actions with respect to punishing employees when their behaviors violate policies is always a difficult subject. There are two schools of thought in this area—the first being one of zero tolerance, where "one strike

and you're out" is the norm. The defense of this view is that in setting the bar high, you get better performers. The downside is that when an otherwise excellent employee makes a mistake, there is no flexibility to save the employee's career or their future contributions to the firm. In an environment where highly skilled workers are not readily available, this lack of flexibility can lead to staffing and morale issues. The second school of thought is to handle adverse issues using the principle "violations will be punished via a range of HR actions, up to and including termination." The flexibility that this offers makes handling cases more challenging because management must determine the correct level of adverse action, but it also provides the flexibility to retain good workers who have made a mistake. Regardless of which path one takes, the key to being legal and ethical is consistency in practice.

Tech Tip

Unintentional Consequences

You should always consider the possible side effects of a policy. For example, I might want to invoke a policy that says only work-related websites are available to employees, with no personal web browsing. I have ways to enforce this at the proxy, so automation is solved. But now I find that the employees only work 9 to 5 and won't stay late. When employees feel less trusted and feel that the organization doesn't care about them, they are less likely to put in the extra effort when it counts the most. As a result, they end up less productive, with low morale. Simple policies can backfire, and the more regulated a worker feels, the more likely they will lose productivity.

Mandatory Vacations

Organizations have provided vacation time to their employees for many years. Few, however, force employees to take this time if they don't want to. At some companies, employees are given the choice to either "use or lose" their vacation time; if they do not take all of their vacation time, they lose at least a portion of it. From a security standpoint, an employee who never takes time off might be involved in nefarious activity, such as fraud or embezzlement, and might be afraid that if they leave on vacation, the organization will discover their illicit activities. As a result, requiring employees to use their vacation time through a policy of mandatory vacations can be a security protection mechanism. Using **mandatory vacations** as a tool to detect fraud will require that somebody else also be trained in the functions of the employee who is on vacation. Having a second person familiar with security procedures is also a good policy in case something happens to the primary employee.

Acceptable Use Policy

An **acceptable use policy (AUP)** outlines what the organization considers to be the appropriate use of company resources, such as computer systems, e-mail, Internet access, and networks. Organizations should be concerned about personal use of organizational assets that does not benefit the company.

The goal of the AUP is to ensure employee productivity while limiting organizational liability through inappropriate use of the organization's assets. The AUP should clearly delineate what activities are not allowed. It should address issues such as the use of resources to conduct personal business, installation of hardware or software, remote access to systems and networks, the copying of company-owned software, and the responsibility of users to protect company assets, including data, software, and hardware. Statements regarding possible penalties for ignoring any of the policies (such as termination) should also be included.

Related to appropriate use of the organization's computer systems and networks by employees is the appropriate use by the organization. The most important of such issues is whether the organization considers it appropriate to monitor the employees' use of the systems and network. If monitoring is considered appropriate, the organization should include

In today's highly connected environment, every organization should have an AUP that spells out to all employees what the organization considers appropriate and inappropriate use of its computing and networks resources. Having this policy may be critical should the organization need to take disciplinary actions based on an abuse of its resources.

a statement to this effect in the banner that appears at login. This repeatedly warns employees, and possible intruders, that their actions are subject to monitoring and that any misuse of the system will not be tolerated. Should the organization need to use in a civil or criminal case any information gathered during monitoring, the issue of whether the employee had an expectation of privacy, or whether it was even legal for the organization to be monitoring, is simplified if the organization can point to a statement that is always displayed that instructs users that use of the system constitutes consent to monitoring. Before any monitoring is conducted, or the actual wording on the warning message is created, the organization's legal counsel should be consulted to determine the appropriate way to address this issue in the particular jurisdiction.

Internet Usage Policy

In today's highly connected environment, employee use of and access to the Internet is of particular concern. The goal of the *Internet usage policy* is to ensure maximum employee productivity and to limit potential liability to the organization from inappropriate use of the Internet in a workplace. The Internet provides a tremendous temptation for employees to waste hours as they surf the Web for the scores of games from the previous night, conduct quick online stock transactions, or read the review of the latest blockbuster movie everyone is talking about. In addition, allowing employees to visit sites that may be considered offensive to others (such as pornographic or hate sites) can open the company to accusations of condoning a hostile work environment and result in legal liability.

The Internet usage policy needs to address what sites employees are allowed to visit and what sites they are not allowed to visit. If the company allows them to surf the Web during non-work hours, the policy needs to clearly spell out the acceptable parameters, in terms of when they are allowed to do this and what sites they are still prohibited from visiting (such as potentially offensive sites). The policy should also describe under what circumstances an employee would be allowed to post something from the organization's network on the Web (on a blog, for example). A necessary addition to this policy would be the procedure for an employee to follow to obtain permission to post the object or message.

E-mail Usage Policy

Related to the Internet usage policy is the *e-mail usage policy*, which deals with what the company will allow employees to send in, or as attachments to, e-mail messages. This policy should spell out whether non-work e-mail traffic is allowed at all or is at least severely restricted. It needs to cover the type of message that would be considered inappropriate to send to other employees (for example, no offensive language, no sex-related or ethnic jokes, no harassment, and so on). The policy should also specify any disclaimers that must be attached to an employee's message sent to an individual outside the company. The policy should remind employees of the risks of clicking links in e-mails or opening attachments, as these can be social engineering attacks.

Social Media Analysis

The rise of *social media networks and applications* has changed many aspects of business. Whether used for marketing, communications, customer relations, or some other purpose, social media networks can be considered a form of third party. One of the challenges in working with social media networks and/or applications is their terms of use. While a relationship with a typical third party involves a negotiated set of agreements with respect to requirements, there is no negotiation with social media networks. The only option is to adopt their terms of service, so it is important to understand the implications of these terms with respect to the business use of the social network.

The use of social media sites by employees at work brings in additional risks, in the form of viruses, worms, and spear-phishing data collection. In years past, employers worried about employees using the machines at work to shop on eBay or surf the Web rather than work. Today, the risks are increased beyond just lost time to now include malware introduction to work machines and devices. It is common for firms to use AUPs to restrict employee personal use of things like social media, peer-to-peer (P2P) networking, BitTorrent, and other non-work-related applications.

Clean Desk Policy

Preventing access to information is also important in the work area. Firms with sensitive information should have a *clean desk policy* specifying that sensitive information must not be left unsecured in the work area when the worker is not present to act as custodian. Even leaving the desk area and going to the bathroom can leave information exposed and subject to compromise. The clean desk policy should identify and prohibit things that are not obvious upon first glance, such as passwords on sticky notes under keyboards or mouse pads or in unsecured desk drawers. All of these elements that demonstrate the need for a clean desk are lost if employees do not make them personal. Training for clean desk activities needs to make the issue a personal one, where consequences are understood and the workplace reinforces the positive activity.

Bring-Your-Own-Device (BYOD) Policy

Everyone seems to have a smartphone, a tablet, or other personal Internet device that they use in their personal lives. Bringing these to work is a natural extension of one's normal activities, but this raises the question of what policies are appropriate before a firm allows these devices to connect to the corporate network and access company data. Like with all other policies, planning is needed to define the appropriate pathway to the company objectives. Personal devices offer cost savings and positive user acceptance, and in many cases these factors make allowing BYOD a sensible decision.

The primary purpose of a BYOD policy is to lower the risk associated with connecting a wide array of personal devices to a company's network and accessing sensitive data on them. This places security, in the form of risk management, as a center element of a BYOD policy. Devices need to be maintained in a current, up-to-date software posture, and with certain

security features, such as screen locks and passwords, enabled. Remote wipe should also be enabled, and highly sensitive data, especially in aggregate, should not be allowed on the devices. Users should have specific training as to what is allowed and what isn't and should be made aware of the increased responsibility associated with a mobile means of accessing corporate resources.

In some cases it may be necessary to define a policy associated with personally owned devices. This policy will describe the rules and regulations associated with use of personally owned devices with respect to corporate data, network connectivity, and security risks. Policies toward mobile device usage are important, as more data usage is happening on these devices. Mobile device deployment models are covered in Chapter 12.

Privacy Policy

Customers place an enormous amount of trust in organizations to which they provide personal information. These customers expect their information to be kept secure so that unauthorized individuals will not gain access to it and so that authorized users will not use the information in unintended ways. Organizations should have a *privacy policy* that explains what their guiding principles will be in guarding personal data to which they are given access.

A special category of private information that is becoming increasingly important today is *personally identifiable information (PII)*. This category of information includes any data that can be used to uniquely identify an individual. This would include an individual's name, address, driver's license number, and other details. An organization that collects PII on its employees and customers must make sure that it takes all necessary measures to protect the data from compromise.

With the intersection of personnel functions (HR) and medical information, enterprises can end up with personal health information (PHI) as well. This information requires safeguards because disclosure can result in legal actions against the enterprise. PHI and PII are covered in Chapter 25.

Cross Check

Privacy

Privacy is an important consideration in today's computing environment. As such, it has been given its own chapter, Chapter 25. Additional details on privacy issues can be found there.

Due Care and Due Diligence

Due care and *due diligence* are terms used in the legal and business community to define reasonable behavior. Basically, the law recognizes the responsibility of an individual or organization to act reasonably relative to another party. If party A alleges that the actions of party B have caused it loss or injury, party A must prove that party B failed to exercise due care or due diligence and that this failure resulted in the loss or injury. These terms often are used synonymously, but **due care** generally refers to the standard of care a reasonable person is expected to exercise in all situations, whereas

due diligence generally refers to the standard of care a business is expected to exercise in preparation for a business transaction. An organization must take reasonable precautions before entering a business transaction or it might be found to have acted irresponsibly. In terms of security, organizations are expected to take reasonable precautions to protect the information that they maintain on individuals. Should a person suffer a loss as a result of negligence on the part of an organization in terms of its security, that person typically can bring a legal suit against the organization.

The standard applied—reasonableness—is extremely subjective and often is determined by a jury. The organization will need to show that it had taken reasonable precautions to protect the information, and that, despite these precautions, an unforeseen security event occurred that caused the injury to the other party. Since this is so subjective, it is hard to describe what would be considered reasonable, but many sectors have a set of "security best practices" for their industry that provides a basis from which organizations in that sector can start. If the organization decides not to follow any of the best practices accepted by the industry, it needs to be prepared to justify its reasons in court should an incident occur. If the sector the organization is in has regulatory requirements, justifying why the mandated security practices were not followed will be much more difficult (if not impossible).

Due Process

Due process is concerned with guaranteeing fundamental fairness, justice, and liberty in relation to an individual's legal rights. In the United States, due process is concerned with the guarantee of an individual's rights as outlined by the Constitution and Bill of Rights. Procedural due process is based on the concept of what is "fair." Also of interest is the recognition by courts of a series of rights that are not explicitly specified by the Constitution but that the courts have decided are implicit in the concepts embodied by the Constitution. An example of this is an individual's right to privacy. From an organization's point of view, due process may come into play during an administrative action that adversely affects an employee. Before an employee is terminated, for example, were all of the employee's rights protected? An actual example pertains to the rights of privacy regarding employees' e-mail messages. As the number of cases involving employers examining employee e-mails grows, case law continues to be established and the courts eventually will settle on what rights an employee can expect. The best thing an employer can do if faced with this sort of situation is to work closely with HR staff to ensure that appropriate policies are followed and that those policies are in keeping with current laws and regulations.

Incident Response Policies and Procedures

No matter how careful an organization is, eventually a security incident of some sort will occur. When it happens, how effectively the organization responds to it will depend greatly on how prepared it is to handle incidents. An **incident response policy** and associated procedures should be developed to outline how the organization will prepare for security incidents and respond to them when they occur. Waiting until an incident happens is not the right time to establish your policies—they need to be designed

Tech Tip

Prudent Person Principle

The concepts of due care and due diligence are connected. Due care addresses whether the organization has a minimal set of policies that provides reasonable assurance of success in maintaining security. Due diligence requires that management actually do something to ensure security, such as implement procedures for testing and review of audit records, internal security controls, and personnel behavior. The standard applied is one of a "prudent person"; for example, would a prudent person find the actions appropriate and sincere? To apply this standard, all one has to do is ask the following question for the issue under consideration: "What would a prudent person do to protect and ensure that the security features and procedures are working or adequate?" Failure of a security feature or procedure doesn't necessarily mean the person acted imprudently.

Due diligence is the application of a specific standard of care. *Due care* is the degree of care that an ordinary person would exercise.

Understanding the differences between due care, due diligence, and due process is important. Due care is having the right policies and procedures, due diligence is checking to see if they are working, and due process is the assurance that all cases go through the appropriate processes.

in advance. The incident response policy should cover five phases: preparation, detection, containment and eradication, recovery, and follow-up actions.

Cross Check

Incident Response

Incident response is covered in detail in Chapter 22. This section serves only as an introduction to policy elements associated with the topic. For complete details on incident response, refer to Chapter 22.

Security Awareness and Training

Security awareness and training programs can enhance an organization's security posture in two direct ways. First, they teach personnel how to follow the correct set of actions to perform their duties in a secure manner. Second, they make personnel aware of the indicators and effects of social engineering attacks.

Many tasks that employees perform can have information security ramifications. Properly trained employees are able to perform their duties in a more effective manner, including their duties associated with information security. The extent of information security training will vary depending on the organization's environment and the level of threat, but initial employee security training at the time of being hired is important, as is periodic refresher training. A strong security education and awareness training program can go a long way toward reducing the chance that a social engineering attack will be successful. Security awareness programs and campaigns, which might include seminars, videos, posters, newsletters, and similar materials, are also fairly easy to implement and are not very costly.

Diversity of Training Techniques

Not all people learn in the same fashion: some learn by seeing, some learn better by hearing. Almost everyone learns better by doing, but in some areas, doing a task is not practical or feasible. The bottom line is that there is a wide range of methods of training, and for the best results it is important to match the training methods to the material. Several different training methods, including gamification, capture-the-flag exercises, and simulations, can be effectively used to improve training. There are even more methods to round out a wide diversity of training solutions, including in-person lectures, online content, and practice-based skill development. The key is to match the material to the method and to the learners, and then test outcomes to ensure successful training has been achieved.

Security Policy Training and Procedures

Personnel cannot be expected to perform complex tasks without training with respect to the tasks and expectations. This applies both to the security

policy and to operational security details. If employees are going to be expected to comply with the organization's security policy, they must be properly trained in its purpose, meaning, and objectives. Training with respect to the information security policy, individual responsibilities, and expectations is something that requires periodic reinforcement through refresher training.

Because the security policy is a high-level directive that sets the overall support and executive direction with respect to security, it is important that the meaning of this message be translated and supported. Second-level policies such as password, access, information handling, and acceptable use policies also need to be covered. The collection of policies should paint a picture describing the desired security culture of the organization. The training should be designed to ensure that people see and understand the whole picture, not just the elements.

User Training

User training is important to ensure that users are aware of and are following appropriate policies and procedures as part of their workplace activities. As in all personnel-related training, two elements need attention. First, retraining over time is necessary to ensure that personnel keep proper levels of knowledge. Second, as people change jobs, a reassessment of the required training basis is needed, and additional training may be required. Maintaining accurate training records of personnel is the only way this can be managed in any significant enterprise.

Gamification

Gamification is the use of games to facilitate user training. This methodology has several interesting advantages. First, it makes rote learning of training material less boring. Second, it enables a more comprehensive situation-based approach to training, with consequences of bad decisions being shared with those taking the training. Third, it allows for group training by using people's job functions in a manner that facilitates both learning and auditing of the policies and procedures in a nonthreatening environment.

Capture the Flag

A **capture-the-flag** event is hands-on computer skill training where users are tested to see if they can perform specific actions. Should they perform the actions correctly, they will uncover a flag that shows they have completed the test successfully. Many hacking competitions are variations of capture-the-flag events.

Phishing Campaigns

Phishing campaigns are a series of connected phishing attacks against an organization. Since phishing is an operational method of social engineering, the greater the level of institutional, organizational, and personal knowledge one possesses about their target, the greater the chance of success. Phishing campaigns use this common knowledge to increase their odds, rather than just randomly attacking targets. This is why internal communications concerning phishing attempts are important: to alert other users

that the system may be under attack and that a heightened sense of awareness toward this form of attack is warranted.

Phishing Simulations

To help users learn and identify phishing attacks, there are methods of running **phishing simulations** against users. A phishing attempt is sent to a user, and should they fall prey to it, the system notifies the user that this was only a drill and that they should be more cautious. This also creates a teachable moment where the user can receive training detailing exactly why they should have spotted the phishing attempt.

Be sure you are familiar with the various user training methods and how they play a role in organizational security. Employ the best method based on circumstances.

Computer-Based Training (CBT)

Computer-based training (CBT) is the use of a computer program to manage training of users. Self-paced modules can facilitate skill development across a wide range of skills, and the flexibility of CBT is very attractive. Not all people learn well under these circumstances, but for those who do, this is a very affordable, scalable training methodology.

Role-Based Training

For training to be effective, it needs to be targeted to the user with regard to their role in the subject of the training. While all employees may need general security awareness training, they also need specific training in areas where they have individual responsibilities. *Role-based training* with regard to information security responsibilities is an important part of information security training.

If a person has job responsibilities that may impact information security, then role-specific training is needed to ensure that the individual understands the responsibilities as they relate to information security. Some roles, such as developer and system administrator, have clearly defined information security responsibilities. The roles of others, such as project manager and purchasing manager, have information security impacts that are less obvious, but these roles require training as well. In fact, the less-obvious but wider-impact roles of middle management can have a large effect on the information security culture, and thus if a specific outcome is desired, training is required.

As in all personnel-related training, two elements need attention. First, retraining over time is necessary to ensure that personnel keep proper levels of knowledge. Second, as people change jobs, a reassessment of the required training basis is needed, and additional training may be required. Maintaining accurate training records of personnel is the only way this can be managed in any significant enterprise.

Data Owner

People who have data responsibilities—whether as a data owner, controller, processor, steward/custodian, or even security specialist—all need specific training in how to respond to these responsibilities. Having training that is targeted to and within the context of a person's responsibilities is easier to assimilate and has better outcomes.

System Administrator

System administrators are administrative users with the responsibility of maintaining a system within its defined requirements. The system owner will define the requirements, such as frequency of backups, whereas the system administrator configures the system to operationally meet these requirements. System administrators have virtually unlimited power over the system—they can control all functions—but what they should not have power over or the responsibility for is the setting of policies for the system. That falls to the system owner.

System Owner

Every system requires a system owner. System ownership is a business function, where the requirements for security, privacy, retention, and other business functions are established. Not all systems require the same policies, but the determination of what the policies for a given system are is the responsibility of the system owner.

User

Normal users need limited access based on their job role and tasks assigned. This is where the principle of least privilege comes into play. Limiting an object's privileges limits the amount of harm that can be caused, thus limiting an organization's exposure to damage. Users may have access to the files on their workstations and a select set of files on a file server, but they have no access to critical data that is held within the database. This rule helps an organization protect its most sensitive resources and helps ensure that whoever is interacting with these resources has a valid reason to do so.

Privileged User

A privileged user has more authority than a standard user. Short of full administrative or root access, a privileged user has permissions to do a wider range of tasks, as their job role may require greater responsibilities. An example would be a database administrator—they would need the equivalent of root access to database functions, but not to all servers or other OS options. Aligning privileges to user responsibilities is good standard policy.

Executive User

Executive users are a special type of user. Their business responsibility may be broad and deep, covering many levels and types of business functions. This work level of responsibilities might not translate directly to their needed computer access. Does the CIO, the highest IT level employee, require all of the permissions of all their subordinates? The true answer is no, because they will not be performing the same level of tasks in their work. And should they on occasion need the access, it can be granted at the time of need.

Limiting the access of executives is not meant to limit their work, but rather limit the range of damage should an account become compromised. Executive users are natural targets for spear phishing attacks, and limiting their system privileges to what is truly needed for them to perform their

system-level tasks thus limits the damage a hacker could cause by compromising an executive account.

Continuing Education

Technology and security practices are far from static environments; they advance every year, and relevant skills can become outdated in as little as a couple of years. Maintaining a skilled workforce in security necessitates ongoing training and education. A continuing education program can assist greatly in helping employees keep their skills up to date.

Compliance with Laws, Best Practices, and Standards

A wide array of laws, regulations, contractual requirements, standards, and best practices is associated with information security. Each places its own set of requirements on an organization and its personnel. The only effective way for an organization to address these requirements is to build them into their own policies and procedures. Training to one's own policies and procedures would then translate into coverage of these external requirements.

It is important to note that many of these external requirements impart a specific training and awareness component on the organization. Organizations subject to the requirements of the Payment Card Industry Data Security Standard (PCI DSS), Gramm-Leach-Bliley Act (GLBA), or Health Insurance Portability Accountability Act (HIPAA) are among the many that must maintain a specific information security training program. Other organizations should do so as a matter of best practice.

User Habits

Individual user responsibilities vary between organizations and the type of business each organization is involved in, but there are certain very basic responsibilities that all users should be instructed to adopt:

- Lock the door to your office or workspace, including drawers and cabinets.
- Do not leave sensitive information inside your car unprotected.
- Keep storage media containing sensitive information in a secure storage device (such as a locked cabinet or drawer).
- Shred paper containing organizational information before discarding it.
- Do not divulge sensitive information to individuals (including other employees) who do not have an authorized need to know it.
- Do not discuss sensitive information with family members. (The most common violation of this rule occurs in regard to HR information, as employees, especially supervisors, may complain to their spouse or friends about other employees or about problems occurring at work.)

- Protect laptops and other mobile devices that contain sensitive or important organization information wherever the device may be stored or left. (It's a good idea to ensure that sensitive information is encrypted on the laptop or mobile device so that, should the equipment be lost or stolen, the information remains safe.)
- Be aware of who is around you when discussing sensitive corporate information. Does everybody within earshot have the need to hear this information?
- Enforce corporate access control procedures. Be alert to, and do not allow, piggybacking, shoulder surfing, or access without the proper credentials.
- Be aware of the correct procedures to report suspected or actual violations of security policies.
- Follow procedures established to enforce good password security practices. Passwords are such a critical element that they are frequently the ultimate target of a social engineering attack. Though such password procedures may seem too oppressive or strict, they are often the best line of defense.
- **User habits** are a frontline security tool in engaging the workforce to improve the overall security posture of an organization.

Training Metrics and Compliance

Training and awareness programs can yield much in the way of an educated and knowledgeable workforce. Many laws, regulations, and best practices have requirements for maintaining a trained workforce. Having a record-keeping system to measure compliance with attendance and to measure the effectiveness of the training is a normal requirement. Simply conducting training is not sufficient. Following up and gathering training metrics to validate compliance and the security posture is an important aspect of security training management.

A number of factors deserve attention when you're managing security training. Because of the diverse nature of role-based requirements, maintaining an active, up-to-date listing of individual training and retraining requirements is one challenge. Monitoring the effectiveness of the training is yet another challenge. Creating an effective training and awareness program when measured by actual impact on employee behavior is a challenging endeavor. Training needs to be current, relevant, and interesting enough to engage employee attention. Simple repetition of the same training material has not proven to be effective, so regularly updating the program is a requirement if it is to remain effective over time.

Standard Operating Procedures

Procedures are the step-by-step instructions on how to implement policies in the organization. They describe exactly how employees are expected to act in a given situation or to accomplish a specific task. Standards are mandatory elements regarding the implementation of a policy. They are

Tech Tip

Reference Frameworks

Industry-standard frameworks and reference architectures are conceptual blueprints that define the structure and operation of the IT systems in the enterprise. Industries under governmental regulation frequently have an approved set of architectures defined by regulatory bodies. Some reference architectures that are neither industry-specific nor regulatory, but rather are technology focused and considered nonregulatory, are the National Institute of Standards and Technology (NIST) Cloud Computing Security Reference Architecture (Special Publication 500-299) and the NIST Framework for Improving Critical Infrastructure Cybersecurity (commonly known as the Cybersecurity Framework, or CSF). It is incumbent on you to understand the appropriate frameworks that apply in the circumstances where you are working.

Tech Tip

Security Training Records

Requirements for both periodic training and retraining drive the need for good training records. Maintaining proper information in security training records is a requirement of several laws and regulations and should be considered a best practice.

accepted specifications that provide specific details on how a policy is to be enforced. Some standards are externally driven. Regulations for banking and financial institutions, for example, require certain security measures be taken by law. Other standards may be set by the organization to meet its own security goals. **Standard operating procedures** are just that: mandatory step-by-step instructions set by the organization so that in the performance of their duties, employees will meet the stated security objectives of the firm.

Third-Party Risk Management

Every business will have third parties associated with their business operations. Whether these third parties are vendors, suppliers, or business partners, they bring the opportunity for both risk and reward. *Third-party risk management* is a fairly straightforward process. The first step is to recognize that risks are present. You need to inventory and assess these risks and then develop the mitigations necessary to keep them in an acceptable range. The important concept is that risk does not magically vanish because a third party is involved; it still needs to be managed like all other business risks.

Vendors

Vendors are firms or individuals that supply materials or services to a business. These items are purchased as part of a business process and represent some form of a value proposition for the firm purchasing them. But with the value can also come risk. For instance, if an item has embedded code to make it operate, what if the embedded code has vulnerabilities? What if an item that is purchased for a specific purpose fails to meet its specifications? A wide range of risks can be introduced by vendors, and these need to be examined and handled in accordance with standard risk management processes.

Supply Chain

A **supply chain** is a set of firms that operate together to manage the movement of goods and services between firms. If you order a part from a foreign supplier that will become part of your product being manufactured in another country, how do all the parts get to the right place for assembly, at the right time? Supply chains handle the details that make all of this happen. From transportation, to customs and other regulations, to managing schedules, these are all details that are necessary for items to go from one place to another. If a firm only has a single supplier, then this process is fairly simple. However, having multiple suppliers of multiple parts at different stages of your value chain that must work together is where supply chains matter. The pandemic of 2020 illustrated this clearly, as countries closed borders, firms had difficulty operating, factories closed due to sick workers and stay-at-home orders—and none of this was uniform or occurred during the same time period. Global supply chain disruptions caused follow-on effects, where expected parts were delayed because

unrelated parts elsewhere were delayed, thus interrupting different supply chains. The need to understand and manage the risks of supply chain functions and their true costs became very evident. It became clear that with extensive supply chain management, lower costs could be achieved, but at the risk of failure when the supply chain had issues.

Business Partners

Business partners are entities that share a relationship with a firm in their business pursuits. Business partners can be enrolled in a business effort for multiple reasons: to share risk, share liability, share costs, leverage specialty expertise, and more. The key to understanding and navigating business partners with respect to cybersecurity and risk is to ensure that the risks and responsibilities on both partners are understood and agreed to before the risk event occurs. With every partnership comes risk and reward; the key is in understanding the level of each and making business decisions with a clear understanding of these elements.

Interoperability Agreements

Many business operations involve actions between many different parties—some within an organization, and some in different organizations. These actions require communication between the parties, defining the responsibilities and expectations of the parties, the business objectives, and the environment within which the objectives will be pursued. To ensure an agreement is understood between the parties, written agreements are used. Numerous forms of legal agreements and contracts are used in business, but with respect to security, some of the most common ones are the service level agreement, business partnership agreement, memorandum of understanding, and interconnection security agreement.

Service Level Agreement (SLA)

A **service level agreement (SLA)** is a negotiated agreement between parties detailing the expectations of the customer and the service provider. SLAs essentially set the requisite level of performance of a given contractual service. SLAs are typically included as part of a service contract and set the level of technical expectations. An SLA can define specific services, the performance level associated with a service, issue management and resolution, and so on. SLAs are negotiated between customer and supplier and represent the agreed-upon terms. Specific security requirements can be specified in an SLA and enforced once both parties agree. Once entered into, the SLA becomes a legally binding document.

Memorandum of Understanding (MOU)

A **memorandum of understanding (MOU)** and memorandum of agreement (MOA) are legal documents used to describe a bilateral agreement between parties. They are written agreements that express a set of intended actions

between the parties with respect to some common pursuit or goal. Typically, an MOU has higher-level descriptions, whereas an MOA is more specific; however, the boundary between these two legal terms is blurry and they are often used interchangeably. Both are more formal and detailed than a simple handshake, but they generally lack the binding powers of a contract. MOUs/MOAs are also commonly used between different units within an organization to detail expectations associated with the common business interest, including security requirements.

Measurement Systems Analysis (MSA)

Many security risk management processes rely on measuring things or events. Measurements and measurement systems have to be calibrated to ensure they are evaluating the actual object of interest. **Measurement systems analysis (MSA)** is a field of study that examines measurement systems for accuracy and precision. Before an enterprise relies on measurement systems, it is important to understand whether the chosen measurement system is acceptable for its intended use, to understand the different sources of variation present in it and to identify and understand sources of bias, errors, and factors associated with repeatability and reproducibility. Performing a measurement systems analysis on the measurement systems employed in a security system is the structured process to get to that information and have confidence in the measures developed and used from the system.

Business Partnership Agreement (BPA)

A **business partnership agreement (BPA)** is a legal agreement between partners that establishes the terms, conditions, and expectations of the relationship between the partners. These details can cover a wide range of issues, including typical items such as the sharing of profits and losses, the responsibilities of each partner, the addition or removal of partners, and any other issues. The Uniform Partnership Act (UPA), established by state law and convention, lays out a uniform set of rules associated with partnerships to resolve any partnership terms. The terms in a UPA are designed as "one size fits all" and are not typically in the best interest of any specific partnership. To avoid undesired outcomes that may result from UPA terms, it is best for partnerships to spell out specifics in a BPA.

Be sure you understand the differences between the interoperability agreements SLA, BPA, MOU, and ISA. The differences hinge upon the purpose for each document.

Interconnection Security Agreement (ISA)

An **interconnection security agreement (ISA)** is a specialized agreement between organizations that have interconnected IT systems, the purpose of which is to document the security requirements associated with the interconnection. An ISA can be a part of an MOU detailing the specific technical security aspects of a data interconnection.

NDA

Nondisclosure agreements (NDAs) are standard corporate documents used to explain the boundaries of company secret material—information that

control over should be exercised to prevent disclosure to unauthorized parties. NDAs are frequently used to delineate the level and type of information, and with whom it can be shared.

End of Service Life (EOSL)

End of service life (EOSL) is the term used to denote that something has reached the end of its "useful life." When EOSL occurs, the provider of the item or service will typically no longer sell or update it. Sometimes the end of updates will be a specified date in the future. EOSL typically occurs because newer models have been released, replacing the older model. During the EOSL phase, some manufacturers may still offer maintenance options, but usually at a premium price. Old versions of software have had this issue, where critical systems cannot easily be upgraded and instead have contracts with the original vendor to maintain the system past its normal EOSL.

End of Life (EOL)

End of life (EOL) or end of support is when the manufacturer quits selling an item. In most cases, while security patches may still be offered, the vendor does not provide for new features or continued compatibility. In some cases, this is announced to be a future date, after which support ends. When something enters the EOL phase, it is at the end of its lifecycle and upgrade/replacement needs to be planned and executed.

Do not be confused! End of life (EOL) is the term used to denote that something has reached the end of its "useful life." End of service life (EOSL) or end of support is when service and maintenance for the solution are no longer provided. In most cases, the manufacturer no longer provides maintenance services or security updates.

Chapter 3 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following regarding operational and organizational security.

Identify various operational aspects to security in your organization

- Prevention technologies are designed to keep individuals from being able to gain access to systems or data they are not authorized to use.
- Previously in operational environments, prevention was extremely difficult and relying on prevention technologies alone was not sufficient. This led to the rise of technologies to detect and respond to events that occur when prevention fails.
- An important part of any organization's approach to implementing security is to establish policies, procedures, standards, and guidelines to detail what users and administrators should be doing to maintain the security of the systems and network.

Identify various policies and procedures in your organization

- Policies, procedures, standards, and guidelines are important in establishing a security program within an organization.
- The security policy and supporting policies play an important role in establishing and managing system risk.
- Policies and procedures associated with human resources (HR) functionality include job rotation, mandatory vacations, and hiring (onboarding) and termination (offboarding) policies.

Identify the security awareness and training needs of an organization

- Security training and awareness efforts are vital in engaging the workforce to act within the desired range of conduct with respect to security.
- Security awareness and training are both important in achieving compliance objectives.
- Security awareness and training should be measured and managed as part of a comprehensive security program.

Understand the different types of agreements employed in negotiating security requirements

- The different interoperability agreements, including SLA, MOU, MSA, BPA, and ISA, are used to establish security expectations between various parties.
- NDA agreements assist in sharing of sensitive information with supply chain, business partners, and other parties that need to use the information.

Key Terms

acceptable use policy (AUP) *(67)*
account disablement *(61)*
account lockout *(61)*
business partnership agreement (BPA) *(80)*
capture the flag *(73)*
change control *(54)*
change management *(54)*
due care *(70)*
due diligence *(71)*
end of life *(81)*
end of service life *(81)*
gamification *(73)*
guidelines *(53)*
incident response policy *(71)*
interconnection security agreement (ISA) *(80)*
job rotation *(63)*
mandatory vacations *(67)*
measurement systems analysis (MSA) *(80)*
memorandum of understanding (MOU) *(79)*
nondisclosure agreements (NDAs) *(80)*
offboarding *(65)*

onboarding *(65)*
phishing simulations *(74)*
policies *(53)*
procedures *(53)*
security policy *(55)*
service level agreement (SLA) *(79)*
standard operating procedures *(78)*
standards *(53)*
supply chain *(78)*
user training *(73)*
user habits *(77)*

Key Terms Quiz

Use terms from the Key Terms list to complete the sentences that follow. Don't use the same term more than once. Not all terms will be used.

1. _____ are high-level statements made by management that lay out the organization's position on some issue.
2. A(n) _____ describes the requisite level of performance of a given contractual service.
3. Mandatory step-by-step instructions set by the organization so that in the performance of their duties employees will meet the stated security objectives of the firm are called _____.
4. _____ are a foundational security tool in engaging the workforce to improve the overall security posture of an organization.
5. _____ are accepted specifications providing specific details on how a policy is to be enforced.
6. _____ generally refers to the standard of care a reasonable person is expected to exercise in all situations.
7. A(n) _____ is a legal document used to describe a bilateral agreement between parties.
8. _____ is used whenever an employee leaves a firm. All associated accounts should be disabled to prevent further access.
9. _____ generally refers to the standard of care a business is expected to exercise in preparation for a business transaction.
10. A(n) _____ is a legal agreement between organizations establishing the terms, conditions, and expectations of the relationship between them.

Multiple-Choice Quiz

1. Which of the following is a description of a business partnership agreement (BPA)?
   - **A.** A negotiated agreement between parties detailing the expectations of the customer and the service provider
   - **B.** A legal agreement between entities establishing the terms, conditions, and expectations of the relationship between the entities
   - **C.** A specialized agreement between organizations that have interconnected IT systems, the purpose of which is to document the security requirements associated with the interconnection
   - **D.** A written agreement expressing a set of intended actions between the parties with respect to some common pursuit or goal

2. What is the name given to mandatory elements regarding the implementation of a policy?
   - **A.** Standards
   - **B.** Guidelines
   - **C.** Regulations
   - **D.** Procedures
3. Which of the following is a contractual agreement between entities that describes specified levels of service that the servicing entity agrees to guarantee for the customer?
   - **A.** Service level agreement
   - **B.** Support level agreement
   - **C.** Memorandum of understanding
   - **D.** Business service agreement
4. During which step of the policy lifecycle does the training of users take place?
   - **A.** Plan for security.
   - **B.** Implement the plans.
   - **C.** Monitor the implementation.
   - **D.** Evaluate for effectiveness.
5. While all employees may need general security awareness training, they also need specific training in areas where they have individual responsibilities. This type of training is referred to as which of the following?
   - **A.** Functional training
   - **B.** User training
   - **C.** Role-based training
   - **D.** Advanced user training
6. Procedures can be described as which of the following?
   - **A.** High-level, broad statements of what the organization wants to accomplish
   - **B.** Step-by-step instructions on how to implement the policies
   - **C.** Mandatory elements regarding the implementation of a policy
   - **D.** Recommendations relating to a policy
7. Which of the following statements are true in regard to a clean desk policy for security? (Select all that apply.)
   - **A.** Although a clean desk policy makes for a pleasant work environment, it actually has very little impact on security.
   - **B.** Sensitive information must not be left unsecured in the work area when the worker is not present to act as custodian.
   - **C.** Even leaving the desk area and going to the bathroom can leave information exposed and subject to compromise.
   - **D.** A clean desk policy should identify and prohibit things that are not obvious upon first glance, such as passwords on sticky notes under keyboards or mouse pads.
8. Key user habits that can improve security efforts include which of the following?
   - **A.** Do not discuss business issues outside of the office.
   - **B.** Never leave laptops or tablets inside your car unattended.
   - **C.** Be alert of people violating physical access rules (piggybacking through doors).
   - **D.** Items B and C.
9. Which of the following is the name typically given to administrative users with the responsibility of maintaining a system within its defined requirements?
   - **A.** System owner
   - **B.** System administrator
   - **C.** Privileged user
   - **D.** Executive user
10. What is the name given to a policy that outlines what an organization considers to be the appropriate use of its resources, such as computer systems, e-mail, Internet, and networks?
    - **A.** Resource usage policy (RUP)
    - **B.** Acceptable use of resources policy (AURP)
    - **C.** Organizational use policy (OUP)
    - **D.** Acceptable use policy (AUP)

Essay Quiz

1. Describe the difference between a BPA and an MOU.
2. Discuss the elements of a good operating procedure.
3. Compare and contrast five HR-related policies with respect to cybersecurity.

Lab Project

• Lab Project 3.1

Describe the four steps of the policy lifecycle. Obtain a policy from your organization (such as an acceptable use policy or Internet usage policy). How are users informed of this policy? How often is it reviewed? How would changes to it be suggested, and who would make decisions on whether the changes were accepted?